

CLAIMS

What is claimed is:

- 1 1. A method of operating a proxy server, the method comprising:
2 receiving an initial request from a user device during a current session
3 between the user device and the proxy server;
4 terminating the current session if the initial request is to a secure server;
5 and
6 establishing a tunnel, through the proxy server, between the user device
7 and the secure server, via a trusted domain proxy/firewall, upon receipt of a
8 further request from the user device to access the secure server if the initial
9 request is to a secure server.
- 1 2. The method of claim 1, further comprising determining whether the initial
2 request is to a destination address of a secure server.
- 1 3. The method of claim 2 wherein determining whether the initial request is to
2 a destination address of a secure server comprises finding a match of the
3 destination address of the secure server in a pre-provisioned list of secure
4 servers in the proxy server.

1 4. The method of claim 2 wherein determining whether the initial request is to
2 a destination address of a secure server comprises forwarding the request to a
3 non-secure server associated with the destination address and receiving an error
4 message in response thereto, which message is indicative that the destination
5 address is that of a secure server.

1 5. The method of claim 1 further comprising waiting a predetermined period
2 for the further request.

1 6. The method of claim 1 wherein establishing the tunnel comprises storing
2 state information in order to identify the further request as being associated with
3 the initial request.

1 7. The method of claim 1 wherein terminating the current session comprises
2 sending an error message to the user device which causes the user device to
3 send the further request to the proxy server.

1 8. The method of claim 7 wherein the error message is a standard error
2 message in a protocol supported by the user device.

1 9. The method of claim 1 wherein establishing the tunnel comprises opening
2 a socket with the trusted domain proxy/firewall and mapping the socket to an
3 inbound socket opened with the user device upon receipt of the further request.

1 10. The method of claim 1 further comprising establishing a time-to-live
2 default for the tunnel, beyond which time the tunnel is terminated.

1 11. The method of claim 1 which comprises terminating the tunnel upon the
2 occurrence of a predetermined event.

1 12. The method of claim 11 wherein the predetermined event comprises
2 receiving a request from the user device to access a server other than the secure
3 server.

1 13. The method of claim 11 wherein the predetermined event comprises the
2 termination of the session between the user device and the trusted domain
3 proxy/firewall at the instance of the trusted domain proxy/firewall.

1 14. A machine readable program storage medium, having code stored therein,
2 which when executed on a proxy server causes the proxy server to perform a
3 method comprising

4 receiving an initial request from a user device during a current session
5 between a user device and the proxy server;

6 terminating the current session if the initial request is to a secure server;

7 and

8 establishing a tunnel, through the proxy server, between the user device
9 and the secure server, via a trusted domain proxy/firewall, upon receipt of a

10 further request from the user device to access the secure server if the initial
11 request is to a secure server.

1 15. The machine readable program storage medium of claim 14, wherein the
2 method comprises determining whether the initial request is to a destination
3 address of a secure server.

1 16. The machine readable program storage medium of claim 15, wherein
2 determining whether the initial request is to a destination address of a secure
3 server, comprises finding a match of the destination address in a pre-provisioned
4 list of secure servers in the proxy.

1 17. The machine readable program storage medium of claim 16, wherein
2 determining whether the initial request is to a destination address of a secure
3 server comprises forwarding the request to a non-secure server associated with
4 the destination address and receiving an error message in response thereto,
5 which message is indicative that the destination address is that of a secure
6 server.

1 18. The machine readable program storage medium of claim 14, wherein the
2 method further comprises waiting a predetermined period for the further request.

1 19. The machine readable program storage medium of claim 14, wherein
2 establishing the tunnel comprises storing state information in order to identify the
3 further request as being associated with the initial request.

1 20. The machine readable program storage medium of claim 14, wherein
2 terminating the current session comprises sending an error message to the user
3 device which causes the user device to send the further request to the proxy
4 server.

1 21. The machine readable program storage medium of claim 20, wherein the
2 error message is a standard error message in a protocol supported by the user
3 device.

1 22. The machine readable program storage medium of claim 14, wherein
2 establishing the tunnel comprises opening a socket with the trusted domain
3 proxy/firewall and mapping the socket to an inbound socket opened with the user
4 device upon receipt of the further request.

1 23. The machine readable program storage medium of claim 14, wherein the
2 method further comprises establishing a time-to-live default for the tunnel,
3 beyond which time the tunnel is terminated.

1 24. The machine readable program storage medium of claim 14, wherein the
2 method comprises terminating the tunnel upon the occurrence of a
3 predetermined event.

1 25. The machine readable program storage medium of claim 24, wherein the
2 predetermined event comprises receiving a request from the user device to
3 access a server other than the secure server.

1 26. The machine readable program storage medium of claim 24, wherein the
2 predetermined event comprises the termination of the session between the user
3 device and the trusted domain proxy/firewall at the instance of the trusted domain
4 proxy/firewall.

1 27. A proxy server comprising:
2 a processor; and
3 a memory device, having stored therein a code, which when executed by
4 the processor, causes the proxy server to :
5 receive an initial request from a user device during a current
6 session between the user device and the proxy server;
7 terminate the current session if the initial request is to a secure
8 server; and
9 establish a tunnel, through the proxy server, between the user
10 device and the secure server, via a trusted domain proxy/firewall, upon receipt of

11 a further request from the user device to access the secure server if the initial
12 request is to a secure server.

1 28. The proxy server of claim 27, wherein the code comprises instructions to
2 determine whether the initial request is to a destination address of a secure
3 server.

1 29. The proxy server of claim 28, wherein determining whether the initial
2 request is to a destination address of a secure server comprises finding a match
3 of the destination address of the secure server in a pre-provisioned list of secure
4 servers in the proxy server.

1 30. The proxy server of claim 29, wherein determining whether the initial
2 request is to a destination address of a secure server comprises forwarding the
3 request to a non-secure server associated with the destination address and
4 receiving an error message in response thereto, which message is indicative that
5 the destination address server is that of a secure server.

1 31. The method of claim 28, wherein the code further comprises instructions
2 for waiting a predetermined period for the further request.

1 32. The proxy server of claim 28, wherein establishing the tunnel comprises
2 storing state information in order to identify the further request as being
3 associated with the initial request.

1 33. The proxy server of claim 28, wherein terminating the current session
2 comprises sending an error message to the user device which causes the user
3 device to send the further request to the proxy server.

1 34. The method of claim 33, wherein the error message is a standard error
2 message in a protocol supported by the user device.

1 35. The proxy server of claim 28, wherein establishing the tunnel comprises
2 opening a first socket with the trusted domain proxy/firewall and mapping the
3 socket to an inbound socket opened with the user device upon receipt of the
4 further request.

1 36. The proxy server of claim 28, wherein the code further comprises
2 instructions to establish a time-to-live default for the tunnel, beyond which time
3 the tunnel is terminated.

1 37. The proxy server of claim 1, wherein the code further comprises
2 instructions to terminate the tunnel upon the occurrence of a predetermined
3 event.

1 38. The proxy server of claim 37, wherein the predetermined event comprises
2 receiving a request from the user device to access a server other than the secure
3 server.

1 39. The proxy server of claim 38, wherein the predetermined event comprises
2 the termination of a session between the user device and the trusted domain
3 proxy/firewall at the instance of the trusted domain proxy/firewall.

1 40. A proxy server comprising:
2 means for receiving an initial request from a user device during a current
3 session between the user device and the proxy server;
4 means for terminating the current session if the initial request is to a
5 secure server; and
6 means for establishing a tunnel, through the proxy server, between the
7 user device and the secure server, via a trusted domain proxy/firewall, upon
8 receipt of a further request from the user device to access the secure server.

1 41. A method of operating a proxy server, the method comprising
2 receiving an initial request from a user device during a current session
3 between the user device and the proxy server;
4 determining whether the initial request is to a secure server;
5 terminating the current session between the user device and the proxy
6 server if the initial request is to a secure server, the current session being

7 terminated with a standard error message in a protocol understood by the user
8 device which message causes the user device upon receipt of the error message
9 to re-send the request to the proxy server; and
10 upon receipt of the re-sent request within a predetermined time, opening a
11 socket with the trusted domain proxy/firewall and mapping the socket with an
12 inbound socket opened between the proxy server and the user device.

Exhibit 4-6-2-6-3